VOLUME 5, ISSUE 5 MAY 2022

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.

Strengthening the Health of Your Business With Cyber Security and Compliance

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

Security and compliance; the terms are often used interchangeably. However, while they are related practices, both are different approaches to a common problem: ongoing cybersecurity threats.

The relationship between compliance and security is best explained with a health analogy. Everyone knows that to stay on top of your game it is important to follow a healthy lifestyle, to eat healthy foods, to exercise, and to be mindful of your physical and mental well-being. However, if you do not know your family's medical history or choose to ignore it, you may still have high cholesterol that requires medication to keep it under control, even with a well-balanced diet.

What Does This Have to Do with Cyber Security and Compliance?

We can all agree that living a healthy lifestyle is a good thing and should be practiced as often as possible. Green vegetables, whole grains, low-fat milk, and exercise are all good stuff, and no doctor would tell you otherwise. But what if you're gluten-sensitive, or lactose intolerant, or you have a bad knee, and running is out of the question? Does healthy living no longer apply?

Of course, it does. You simply have to make adjustments. Living a healthy lifestyle will prevent sickness and health issues, but what healthy eating is for you might not be quite the same as for your gluten-sensitive, lactose-intolerant friend. The concept remains, only the tools to get there are slightly different.

The same applies to compliance and security. While there is some overlap, both compliance and security are necessary for the healthy operations of your business. Whereas compliance helps you

maintain an "audit-ready" posture, your security tools are what allows you to sustain a "low-risk" outlook from a security perspective.

Let me explain.

Cyber security is a set of techniques and practices that you put in place to protect your digital infrastructure and electronic data from being compromised by cyber-attacks. Whatever those measures are is dictated by how you run your business, the type of data you collect, where it resides, who has and needs access to it to perform their job, and where this might result in vulnerabilities that need to be protected.

Whereas cybersecurity includes all the tools, processes, and operations needed to protect data, **compliance** aligns those security systems within the standards set by a governing body to call for a basic level of security for all businesses.

Over the past ten years, over 10,000 regulations have been placed on the books by local, state, and federal agencies pertaining to the handling, storage, and disposal of digital personal information (PII/PHI).

A few examples are:

- SEC Rule 17a-4 Electronic Storage of Broker-Dealer Records Graham-Leach-Bliley Act
- DOD 5015.2 Department of Defense
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security (PCI DSS)
- Gramm-Leach Bliley Act (GLBA)
- NY State Data Protection Act (SHIELD)
- Defense Federal Acquisition Regulation Supplement (DFARS)

No matter how small your business is, you will undoubtedly be affected by one or more of these government regulations. Naturally, some industries are more regulated, such as financial or medical. Still, all companies that hold information such as employee social security numbers, credit cards, financial statements (credit applications, bank statements, order forms) fall under at least one of these regulations:

- Providers in the healthcare industry, you must follow HIPAA compliance. **HIPAA** is a federal law that aids in the privacy of patients' health records. It imposes rules and regulations on healthcare providers and companies within the field to keep patients' private health information (PHI) from being disclosed without their consent or their knowledge.

- Providers in the Defense Industry or working with Department of Defense agencies must meet **NIST 800-171, and DFARS** (soon to be supplemented by or replaced by **CMMC**) standards as these contractors often have access to information that is classified or not public.

- Any organization managing credit card payments need to adhere to **PCI-DSS**, which governs how you handle customer credit card data at the point of sale, data transfers, and data at rest in a server.

- Compliance regulations for those who operate in the financial industry are some of the strictest around. Not only are you subject to the **Gramm-Leach Bliley Act**, but you are also regulated by the **Sarbanes-Oxley Act (SOX)** and, if you happen to operate in the state of New York, NYDFS 500 regulations.

- To make things more complicated, regardless of your business vertical (or the subsequent compliance rules you need to adhere to) or size of your business, all of us who collect or have access to data on NY state citizens are subject to the New York **SHIELD Act** (or Stop Hacks and Improve Electronic Data Security Act). This act requires any business or individual that owns or licenses computerized data on NY residents to maintain the safeguards necessary to protect their sensitive information.

In other words, compliance dictates standards and outlines blueprints (i.e., what constitutes a healthy lifestyle), that force organizations to make cybersecurity an essential part of their business operations (healthy foods and exercise are fundamental to that healthy lifestyle). What specific security measures are appropriate for your business depends on size, vertical, and the kind of data you must protect (i.e., family history, body type, etc.).

Cyber security and compliance work right alongside each other. If you're trying to ensure that your business stays compliant, you need to buff up your cyber security practices. There are many methods you can take to do this, but if you're unsure of where to begin, give us a call. We would be glad to help you take the next steps toward creating a cyber-secure business.

All you need is a health coach to help you get started and remain on track.

Are you still running your business from your office?

Surprisingly, I'm NOT talking about hybrid or remote workers.

Instead, the question in the headline refers to your servers, your systems, and your network. Are they all in-house? Or have you – like countless other businesses – moved everything over to the cloud yet?

Migrating your business systems to the cloud can be a big and scary process. Then why are we seeing

so many companies doing it?

That's simple - there are SO many benefits.

First, it saves you money. That's because you only pay for the data you need rather than having a little bit more 'just in case'. And it means that your systems won't hold you back as your business grows.

But then there's the security aspect too. When you migrate to cloud services you benefit from a higher level of protection against data breach and theft. Plus, cyber security aside, if you had a disaster in the office such as a burglary or a fire, you'd know your data is safe.

Of course, it's a tricky process and there's a lot of planning involved. But if you're working with an expert to make the transition, you can rest assured that things will go to plan.

We recently wrote a guide to cloud migration. It goes into more detail about the pros and cons of moving your business to the cloud. Would you like a copy? Just drop us an email at info@meetingtreecomputer.com and we'll send it over to you.

In a recent report, 63% of businesses said they'd had a security breach as a direct result of a member of their team side-stepping security measures.

Doh.

Ongoing Security Awareness Training is key in a robust cybersecurity program. To help your team make smart cyber security decisions, they need ongoing training to understand why security measures are in place and improves their ability to spot scams and detect possible cyber-attacks.

How often does your business talk openly about cyber security? How often do you provide formal training for them?

Your Tech Tip of the Month

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that provides minimum requirements for protecting certain health information.

Because of the kind of information HIPAA protects, the penalties can be quite severe—even unknowing or accidental violations can result in fines up to $50,000 per violation.

If your health organization handles sensitive and personal data, you'll want to know about the most common HIPAA compliance issues and how to address them:

https://bit.ly/MTC-TT77-Most-Common-HIPAA-Compliance-Issues

Top 5 Tips for QR Code Safety

As the pandemic restricted the touching and sharing of physical objects, QR codes have become a regular staple in our lives.

Unfortunately, as the codes have become an increasingly helpful addition to our lives, scammers have been working hard to use this to their advantage.

But don't fear. Here are five tips to help keep you safe:

Check the URL: When scanning a QR code, a preview of the website link is displayed prior to you clicking it. If the link looks short or is unrecognizable, be cautious to move forward. Only use links that will take you exactly where you expect to go.

Double-check the URL: Once you tap on the QR link, make sure that it takes you to the website you were expecting and not a clever phishing site that looks like an exact copy of it. Beware of the details!

Do not log into any accounts: After clicking on a QR code, be careful about using login information on these sites. Sometimes it will be necessary to do so but be wary of sharing any personal information to websites that you access through a QR scan.

Never download apps: A very common scam is creating a QR code that lures you into downloading a fun-looking app while, in reality, it is installing malware and stealing your personal information. All the fun goes to the attacker and none for you! Our advice: avoid downloading applications to your device when it stems from a QR code. Download through the app store instead.

Limit payments made: Unless you are sure, that it is legitimate and the payment is through a reliable company, do not make payments through QR codes. In other countries it is less common to use QR codes for payment, so be careful, especially if you are traveling.

Remember, not all QR codes are dangerous. They are essentially links. As long as you stay alert and follow these 5 tips you are ready to scan away.

2 Ways to Use Technology as Part of Your Business Growth Strategy

May is a big course correction month. Hopefully the first half of the year has gone as planned, new initiatives have been implemented and you now have time to focus on the more supportive projects of your operations.

We call this the May Refresh & Refocus.

We see two technology areas that will be the most important for the remainder of 2022: Defend and Invest.

Defend is about protecting your business from cyber criminals as cyber-crime is has been rising again to levels never seen before. Invest is about making sure technology is powering your business forward, not holding it back.

Our new guide looks at both these areas in detail:
https://www.meetingtreecomputer.com/files/2022/04/Defend-Invest-Guide.pdf

How does speech recognition work?

Software breaks down your speech into individual sounds, then analyses them using algorithms to find the most probable word that fits. It will also look at sentence structure that humans typically use.

How can I make my passwords more secure?

Use a password manager.

It will generate and store long strong random passwords for all your accounts. We can recommend the best one for your business.

Is a paperless office really better for security?

While paper documents are impossible to steal remotely, once they are lost there's no chance of recovery. Go paperless and invest in a good backup… just make sure your IT partner is regularly checking its working properly.

Submit Your Question Here:

mduci@meetingtreecomputer.com

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us